Cloud Security VS Cybercrime Economy: The Kaspersky Vision

Eugene Kaspersky
Co-founder & CEO, Kaspersky Lab
The Digital World is Under Attack

Cybercrime is an integral part of the Digital World.

Cybercrime is an organized underground industry.

The last five years have become the Golden Age of Cybercrime.

Number of new malicious programs found by Kaspersky Lab every year:

- 2004: 0
- 2005: 0
- 2006: 0
- 2007: 2,000,000
- 2008: 4,000,000
- 2009: 6,000,000
- 2010: 18,000,000
Why is it happening?

It’s profitable

- More online services that are easy to prey on
- High demand for criminal services (spam, botnets)

Easy to do

- It’s simple – technically speaking
- No physical contact with victims

Low risk business

- International crime vs. national legislation
- Difficult to trace anonymous international professionals
Main types of malware businesses

There are many different malware businesses:

- Common: banking, ransom, botnets, etc.
- Targeted attacks – Aurora, Stuxnet, Night Dragon
- Exclusive: Sumitomo £229mln., NYSE Trojan attacks
- Mobile attacks: Spyware, SMS-Trojans, Backdoors

Some criminal businesses are born –
ATM malware, mobile attacks

Some criminal businesses vanish
Dial-up, online game malware
Examples of malware businesses

Special of Specials


Special of Specials

Examples of malware businesses

But today it goes down due to the inflation on the black market of online game characters and artifacts
ERGO –

The main motivation for cybercrime growth is its economical profitability

Profit decline decreases malware of that type
A standard malware business scenario

Malware lifetime

- Development and placement (usually on Web)
- Distribution (spam, Web-site infection)
- Injection and infection
- AV products updated
- the end
A standard malware business scenario

Malware lifetime

- Development and placement (usually on Web)
- Distribution (spam, Web-site infection)
- Injection and infection
- AV products updated
- the end
The Era of Happy Cybercriminals

Is there anything that can stop it?
The Principle of Cloud Security

KL

co

ce

nputers in

Th

the

Th
Instead of making a lot of cash, cybercriminals earn much less, or ever lose money
“Cloud” security becomes new industrial standard

- KLOud Security Network (Kaspersky)
- Quorum (Symantec)
- Global Threat Intelligence (McAfee)
- Smart Protection Network (Trend Micro)
- Others are joining the team.
Silver bullet?

Ways to bypass the “cloud”:

• Non-executable malware
• Server-side polymorphic malware
• File infectors
• New behavior

• Simple malware is blocked by KLoud Security in a few minutes
• The rest is tackled by traditional AV Technologies
Conclusion

KLoud is not the Silver Bullet, but:

• It makes malware hard to develop and unprofitable
• The entrance ticket to Cybercrime becomes more expensive

KLoud is a quick solution for suppressing cybercrime!

Happy End!
Thank You

Cloud Security VS Cybercrime Economy: The Kaspersky Vision

Eugene Kaspersky
Co-founder & CEO, Kaspersky Lab